CENTER FOR
CYBERSECURITY
POLICY AND LAW

WHITEPAPER

MEETING THE HOMELAND C-UAS THREAT

Jennifer Daskal, Davis Hake, Tim McGiff

DECEMBER 2025

Executive Summary

> *A swarm of small commercial drones laden with explosives descended on the attendees departing the local university hockey game in the town of "Minor Spoon," North Dakota, leaving multiple dead and more wounded. Another swarm attacked the electric grid, causing a power outage across the entire town and surrounding area. The nearby air base suffered considerable damage from a third wave of attack. First responders faced a city in panic and a mass casualty event that seemingly came out of nowhere. . .*

This was the hypothetical scenario laid out by the Center for Cybersecurity Policy and Law during a three-hour exercise in Grand Forks, North Dakota, on October 13, 2025. Over the course of an afternoon, participants from local, state, and federal governments, along with private industry, higher education, and representatives from key energy providers, responded to hypothetical attacks on the air base, electricity grid, and a local hockey game in the fictitious town of "Minor Spoon."

Sound far-fetched? Over the past several months, drone sightings in Europe have led to multiple airport shutdowns.[1] During the Paris Olympics, authorities reported an average of six unauthorized drone incursions each day.[2] Drones also have crashed into the seating areas at the U.S. Open and a Major League Baseball game, luckily with no injuries.[3] Ukraine's drone attack on strategic air bases deep inside Russia as part of Operation Spider Web also provides a stark reminder of the vulnerabilities in places otherwise deemed secure.[4] The low cost of drones makes them a potentially powerful and pervasive weapon.

Exercise participants grappled with both the threat and response options. Participants were broken into four teams: the Minor Spoon Air Base, the Minor Spoon Electric, the Minor Spoon University, and the Minor Spoon city government. Over three rounds, the teams were tasked with:

- Responding to threat briefings that included inchoate warnings about a potential, impending attack;
- Reacting to an attack that caused loss of life, injuries, and damage to property; and
- Engaging in recovery actions, while still facing the possibility of follow-on attacks.

---

[1] Jenny Gross, What We Know About the Drone Sightings in Europe, New York Times (Oct. 22, 2025), https://www.nytimes.com/2025/10/22/world/europe/drone-sightings-airports.html

[2] France 24, French security forces intercept six drones a day near Olympics sites, PM says, France 24 (Jul. 23, 2024), https://www.france24.com/en/europe/20240723-french-security-forces-intercept-six-drones-a-day-near-olympics-sites-pm-says

[3] Julia Talanova, Drone slams into seating area at U.S. Open; teacher arrested, CNN (Sep 5, 2015), https://www.cnn.com/2015/09/04/us/us-open-tennis-drone-arrest; Marissa Payne, MLB will 'monitor the situation' after drone nearly takes out fans at Padres game, Florida Times-Union (May. 24, 2017) https://www.jacksonville.com/story/news/nation-world/2017/05/24/mlb-will-monitor-situation-after-drone-nearly-takes-out-fans-padres-game/15756400007/

[4] Laura Gozzi, BBC Verify, How Ukraine carried out daring 'Spider Web' attack on Russian bombers, BBC News (Jun. 2, 2025) https://www.bbc.com/news/articles/cq69qnvj6nlo

The teams worked collectively to identify actions that would best ensure the safety and well-being of the local population, minimize damage to property, and lead to a better understanding of the source of the attacks and potential for future attacks. At the conclusion of the exercise, participants convened to discuss their key takeaways and recommendations for preparing and responding to a potential drone threat.

Among the key findings:

1. **Effective detection is key.**
   Without effective detection, there is no way to assess whether reported drone sightings are actual drones (versus birds, other aircraft, or mis-sightings), and, if so, whether they are likely hobbyist drones or drones associated with sophisticated malicious actors.
2. **Effective detection is hindered by several limitations,**
   including a lack of baseline mapping of what is "ordinarily" in the airspace, resource constraints, confusion about the kinds of detection measures permitted under current law, and legal restrictions on engaging in certain advanced detection measures that interact with the communication signal between a drone operator and the drone.
3. **Far too few actors have authorities to effectively counter the drone threat.**
   Only a handful of federal government actors—the departments of War, Energy, Justice, and Homeland Security—are authorized to engage in drone mitigation, and even these authorities are limited to protecting certain assets and facilities. State and local officials and critical infrastructure owners do not have affirmative authority to engage in active detection measures that engage the communication system between the drone operator and drone, let alone any mitigation measures.
4. **Counter-drone measures need to be integrated into core security planning.**
   Management of the threat posed by the malicious or negligent use of drones needs to be integrated and normalized as part of core security planning. Conversely, management of the drone threat should incorporate key elements of crisis management and prevention, regardless of the source of the threat. In the wake of an attack, there is a need for rapid deployment of emergency services, crowd control, engagement across local, state, and federal authorities, smart and effective communications, and strong organizational structures. Longer term, there are likely to be oversight demands, litigation risks, and the need for rebuilding and rebranding.[5]

The following paper describes the exercise in more detail, including findings and associated recommendations for increased resources, authorities, education, and planning to address the threat.

[5] Desiree F. Moore, Jennifer Daskal, Christopher R. Obrien, Sports Lawyers Emphasize Crisis Preparedness and Legal Readiness Amid Growing Risks, Venable LLP (Oct. 17, 2025), https://www.venable.com/insights/publications/2025/10/sports-lawyers-emphasize-crisis-preparedness

The Exercise: Details and Results

Over three hours, teams representing an air base, university, energy sector critical infrastructure, and local government responded to a dynamic and escalating series of hypothetical drone attacks. In the first round, participants responded to social media reports of unidentified drones being sighted around the city, coupled with warnings from federal sources about social media chatter indicating a heightened threat environment. In the second, they reacted to the attack itself, made more difficult by a power outage in the North Dakota winter. And in the third, they engaged in recovery actions the day after the attack, while still facing the possibility of follow-on attacks. Each team was forced to struggle with limited knowledge, authorities, and resources as they collectively charted the best course of action in light of these limitations.

Scenario

The exercise was set in the fictional city of Minor Spoon, North Dakota, a town with a population of about 70,000 near the border with Minnesota. This fictional town has an international airport, a university, a coal power plant, and an air force base, all within a 20-mile radius.

The Teams

Participants were broken into the following four teams:

- **Minor Spoon Air Force Base,** which houses 3,500 civilian and active-duty military personnel, operates and maintains several dozen RQ-9 Reaper aircraft and is located about 15 miles outside of Minor Spoon. Participants represented the base's leadership and security personnel.
- **Minor Spoon University,** a major research university with approximately 15,000 students located approximately four miles outside of the city center of Minor Spoon, and with a particular point of pride in the school's very strong hockey team. Participants represented university leadership, security teams, and athletic directors.
- **Minor Spoon Electric,** the primary entity responsible for producing and distributing power to the Minor Spoon area, most of which comes from a coal plant located 20 miles west of the city. Participants represented executives and emergency response teams based out of the local headquarters.
- **Minor Spoon Government,** which represents all Minor Spoon residents. Participants included representatives from the mayor's office, local law enforcement and emergency responders, regionally based Customs and Border Protection officials, and state officials.

Scene Setter

Participants were provided a read-ahead that set the following background conditions for the exercise. (Note: The full scene setter is included in Appendix B.)

Local news and social media had been reporting an unusual number of drone sightings in the area. National news started to report on the "drones in Minor Spoon," and the governor and mayor's office have been fielding calls from concerned citizens.

Earlier in the month, the Cybersecurity and Infrastructure Security Agency alerted civilian critical infrastructure owners and operators of what appears to be increased cyber activity/attempts to penetrate the networks of critical infrastructure across the region.

A few days earlier, the local FBI field office also reached out to campus security officers across the United States, warning of increased online chatter expressing support for an attack that targets students. No specific threat actors or targets were identified.

Round One

The first round took place late afternoon on a hypothetical Friday. Each team received information about an unusual number of drone sightings, along with intelligence reports indicating unconfirmed warnings of a potential attack.

The following summarizes the information provided to each team and the responses:

1. ***Minor Spoon Air Force Base:*** *There are unconfirmed sightings of drones flying into protected airspace over the base and intelligence reports warning of an increased threat level and non-specific efforts to target the base's MQ-9 reapers. At 4:30 p.m., the Commander learns of new drone sightings at the base fence line…*
    - The team focused on information gathering—including reaching out to local, regional, and national partners to learn more about the reports and whether the activity was isolated or part of a larger trend.
    - The team discussed, with some frustration, the lack of authority to engage directly with the drones or their operators or otherwise take action to mitigate the threat so long as the drones were operating outside of the base perimeter.
2. ***Minor Spoon University:*** *Social media is abuzz with reports of multiple drone sightings later that evening. The university hockey team is playing a sold-out game with its key rival. A 4:30 p.m. call from the local FBI field office warns of online chatter expressing support for an attack that targets students. Doors open in one hour…*
    - Like the Air Base team, the University team prioritized information gathering. They discussed whether to cancel the game but ultimately determined that they lacked sufficiently credible information to do so.
    - The team instead sought to coordinate with local law enforcement on a threat response and threat mitigation plan. They were surprised to learn that local law enforcement lacked resources to track the drones and lacked authority to redirect the path of or otherwise mitigate a potentially threatening drone.

3. ***Minor Spoon Electric:*** *There are reports of increased drone activity in the region and a potential threat. A 4:30 p.m. report indicates that two drones have been hovering over the Minor Spoon Power Plant for the last 30 minutes…*
    - The team focused its attention on information gathering, to include communication with internal personnel and external partners to better assess any potential threat.
    - As with the University team, the Electric team was frustrated by the lack of resources to track reported drones and there was a general consensus that not enough information was known about the anomalous drone activity to trigger additional action.
4. ***Minor Spoon Government:*** *The government team receives a collection of the intelligence reporting provided to other teams…*
    - The team focused on the information challenges, given a lack of clarity as to whether reported drone sightings were negligent or malicious.
    - The team also discussed the limited resources available to detect and the limited authorities to respond to potentially concerning drones. While Customs and Border Protection noted that they could send detection and mitigation tools to support the city, it would take some time to coordinate and provide the needed resources.

Round Two

The second round took place several hours later, at around 9:30 p.m. in the evening. The air base, university, and power plant were all hit by drone swarms—causing casualties, panic, and physical/infrastructure damage.

The following summarizes the information provided to each team and the responses:

5. ***Minor Spoon Air Force Base:*** *External power to the base is cut off. Minutes later an estimated two dozen drones target aircraft on base, the air traffic control tower, the on-base electrical substation, fuel storage area, and Air Base fire department…*
    - Leveraging prior training, the team prioritized force protection, damage containment, command continuity, and assessment of mission-critical assets.
    - Given the widespread nature of the attack, the team focused internally. The team recognized the base could not rely on normal community assistance and would need to operate independently. Conversely, the base would have to withhold typical community support given the need to focus on protecting base personnel, core missions, and preserving combat readiness.
6. ***Minor Spoon University:*** *Just after the hockey game ended, electricity goes out. Minutes later, there are several explosions. Videos show drones dropping explosives on departing fans, causing what appear to be multiple casualties and injuries…*

- The team focused on emergency response.
- The team decided to activate the emergency alert systems but debated whether to require students to shelter in place or encourage them to leave the area. (Participants were divided.)
- The team also emphasized the importance of coordination with others, including the hospital to prepare to receive patients, local law enforcement to help with crowd control and protect against future attacks, and the fire department to respond to the fires.

7. ***Minor Spoon Electric:*** *The Manager of the Minor Spoon Power Plant reports numerous drone strikes, resulting in disruption to all external power. Several personnel report minor injuries and three personnel are unaccounted for…*
    - The team prioritized employee safety. While the team discussed the need for damage assessment and recovery, they decided that their primary, initial focus needed to be on personnel safety.
    - The team recognized they lacked counter-drone capabilities and authorities and made the decision to require personnel to shelter in place.
8. ***Minor Spoon Government:*** *Power is out, social media and others report drone attacks on the University, power plant, and Air Base. The phones are ringing, as are state and local officials trying to find out what has happened, and reporters are asking for comments…*
    - The team focused on emergency response and emphasized the importance of triaging to support those places with the greatest need.
    - The team decided to require city residents to shelter in place, provide emergency shelters for those who need them, and reach out to Customs and Border Protection and the local Air Base for support in detecting and mitigating future attacks.

Round Three

The final round took place early the following morning as the teams worked through coordination and implementation of recovery operations.

9. ***Minor Spoon Air Force Base:*** *Several civilians on base suffered injuries and three remain in critical condition. There is significant damage to one MQ-9 Reaper and one aircraft. Fires on the base have been put out but there is still no electricity on base. Social media claims more attacks are coming. Local authorities are seeking support and press is asking for comment…*
    - The team turned to stabilization and information management. The team prioritized maintenance of operational command, restoration of internal power, and provision of medical care to the wounded.
    - Participants discussed the importance of clear, unified messaging to prevent the spread of misinformation.

- The team also highlighted the need for additional intelligence about the threat, and reached out to local, regional, and national partners to learn if the activity was isolated or part of a larger trend.

10. ***Minor Spoon University:*** *There are a dozen confirmed deaths and multiple others in critical condition. The hockey arena has been hit, but the fires have been extinguished, and the area is clear. Electricity is still out. Reports indicate there may be follow-on attacks. Concerned parents are calling…*
    - The team continued to focus on the well-being of students, faculty, and staff.
    - The team remained very concerned about potential follow-on attacks, along with the many challenges to effectively responding, given limited resources and authorities.
11. ***Minor Spoon Electric:*** *Three previously accounted-for personnel were hit in the attack. One is deceased, the other two are in critical condition. Production and transmission of electricity continues to be severely limited, and personnel responsible for damage assessment and repair are concerned about follow-on attacks…*
    - The team began to focus on assessment and recovery but remained deeply concerned about potential follow-on attacks and the limited capacity and authority to protect personnel and equipment.
    - The team decided to hold most assessment and recovery work until they had been guaranteed adequate protection from law enforcement, National Guard troops, or otherwise.
12. ***Minor Spoon Government:*** *There are multiple casualties throughout Minor Spoon and at the nearby air base. Electricity is still out, and now all flights in and out of the regional airport are grounded. Social media reports more attacks are coming. State and federal authorities are asking for information and offering support. The press keeps calling…*
    - The team focused on recovery, to include the following:
        - Provision of support for families of the deceased and wounded;
        - Requests for drone detection and mitigation support from federal authorities;
        - Law enforcement activity and presence to protect against looting; and
        - Regular coordination communication with community members and the press.

Findings and Recommendations

At the conclusion of the three rounds, the teams convened to discuss their reactions, broader concerns, and recommendations—which are incorporated into the findings and recommendations that follow:

1. Strong Counter-Drone Measures Are an Essential Part of an Effective Domestic Drone Growth Strategy

There are over eight hundred thousand drones registered with the FAA in the United States—a likely undercount of the number of drones actually in the U.S. skies—and a number that is predicted to grow to close to three million by 2027.[6] The lawful use of drones generates significant commercial, economic, public safety, and recreational benefits. Drones are used to support firefighters, the delivery of life-saving aid, critical infrastructure management, agricultural production, and military operations, along with multiple other commercial and recreational uses. As technology evolves, so will the benefits. Our domestic drone industry thus plays a key and expanding role in the current economy.

But growth without sufficient protections carries risks. One needs to read only a few headlines about the fighting in Ukraine and across the Middle East to know that relatively inexpensive and off-the-shelf technologies can be adapted for military use. Drones have been used in assassination attempts, including those of the president of Venezuela and the prime minister of Iraq.[7] [8] Transnational criminal organizations use drones to smuggle deadly drugs across our southwest border and into our prisons. Drones can be used by foreign adversaries for espionage purposes, including to collect intelligence on targets of interest. Drones also have posed serious safety risks to airports, critical infrastructure, and large public gatherings like football games.

Safe and secure growth of the domestic drone industry requires effective counter-drone measures to both identify and combat negligent and malicious drone use. Counter-drone measures are thus a core element of a strategic and affirmative drone-growth strategy.

2. Effective Air Space Awareness is a Key First Step to Protection

The exercise highlighted the challenges in identifying a potential threat—the first step in enabling an effective response. When participants received information about reported drone sightings, they lacked both resources and authorities to engage in the kind of advanced detection needed to determine if, in fact, the reports were accurate, and if so, whether the reported sightings were normal hobbyist behavior or indicative of an active

---

[6] Federal Aviation Administration, Drones by the Numbers (as of November 2025), Federal Aviation Administration (Dec 8, 2025)https://www.faa.gov/node/54496; Government Accountability Office, Drone Operations, *Government Accountability Office* (Dec. 18, 2025) https://www.gao.gov/drone-operations.

[7] Iraqi PM al-Kadhimi survives drone attack on his home, *BBC* (Nov. 7, 2025) https://www.bbc.com/news/world-middle-east-59195399

[8] Venezuela President Maduro survives 'drone assassination attempt', *BBC* (Aug. 5, 2018), https://www.bbc.com/news/world-latin-america-45073385

threat. Many participants were also unsure as to the kinds of detection measures they could undertake without running afoul of applicable legal restrictions.

This leads to the following three recommendations:

a. **Importance of Airspace Mapping:** There is no broadly available mapping of the low-altitude airspace where drones generally operate. This is critical to creating a baseline understanding of what is normally in the skies, identifying anomalies, and distinguishing between lawful, negligent, and malicious use of drones. The Federal Aviation Administration (FAA) should be authorized and resourced to create this mapping in coordination with private sector partners and required to make this information available to state and local partners.

b. **Local Officials, Critical Infrastructure Owners and Operators, and Other Private Actors That Support Mass Gathering Need More Resources and Expanded Authorities:** Currently, state and local officials, critical infrastructure owners and operators, and others that bring together large numbers of people need clarity about the kinds of permitted detection authorities, increased investment in such detection measures, and additional authority to engage in the kind of active detection that can detect unlawfully present drones that fail to operate with the required remote ID or emit detectable signals.

   Local officials and private sector operators can lawfully engage in a range of passive detection measures, such as tracking signals that drone operators emit. That said, many are constrained by a lack of resources and lack clarity as to the scope of permitted detection measures. Moreover, such detection will not capture sophisticated malicious drone users that do not emit such signals.

   The One Big Beautiful Bill passed by the 119th U.S. Congress seeks to address some of the resource challenges. It creates a $500 million grant program that explicitly supports state and local officials' efforts to purchase detection equipment and put in place a stronger C-UAS program.[9] A separate $625 million FIFA World Cup Grant Program can also be used to purchase UAS detection and tracking equipment.[10] Current grant allocations are, however, limited to the 11 states where the 2026 FIFA World Cup will be held. More resources and a broader geographic reach are needed to support additional state and local officials across the nation.

c. **Expanded Advanced Detection Authorities Are Also Needed:** Only a handful of federal agencies—the departments of War, Energy, Justice, and Homeland Security—are explicitly exempt from relevant provisions in the Pen/Trap Statute and

[9] Federal Emergency Management Agency, Notice of Funding Opportunity (NOFO) Counter-Unmanned Aircraft Systems (C-UAS) Grant Program, Federal Emergency Management Agency (Nov. 12, 2025), https://www.fema.gov/fact-sheet/notice-funding-opportunity-nofo-counter-unmanned-aircraft-systems-c-uas-grant-program

[10] Federal Emergency Management Agency, FIFA World Cup Grant Program, Federal Emergency Management Agency (Nov. 12, 2025), https://www.fema.gov/grants/preparedness/fifa-world-cup-grant-program

Wiretap Act can engage in the kind of active detection that engages the communication between drone operator and drone that otherwise trigger restrictions, and can therefore help identify drones that are not operating with the required remote ID. But these authorities are limited to specific "covered assets" and limited geographic areas.

There is an urgent need to expand the federal government's authorities, including by making explicit the Department of War's authority to engage in active detection outside the base perimeter, and to also grant state and local officials the authority to engage in advanced detection. As discussed below, provisions included in the House of Representatives-introduced National Defense Authorization Act for Fiscal Year 2026 (2026 NDAA) would make several of these key changes.[11]

d. **Temporary Flight Restrictions Are Helpful Tools:** Temporary flight restrictions are helpful, as they enable clear identification of unlawful drone use—namely any non-approved drone inside the restricted airspace. The FAA has indicated an intent to issue a new rule (known as the "2209 Rule") that would enable critical infrastructure owners and operators and entities that bring together large numbers of people to more easily request and obtain such restrictions. This would better support detection and appropriate response efforts. The FAA should expedite issuance of this new rule.

3. There is an Urgent Need for Additional Authorities and Resources to Mitigate Identified Threats

The exercise also highlighted the limited authorities and resources to mitigate an active drone threat, leading to the following recommendations:

a. **Need for Expanded Mitigation Authorities:** The same four federal agencies—the Departments of War, Energy, Justice, and Homeland Security—that are exempt from federal laws that limit certain detection methods also are the only agencies authorized to engage in mitigation of drone threats.[12] And, as described above, this authority is significantly circumscribed to the coverage of certain "covered assets" and geographic areas. There is no authorization for agencies to engage in cross support of one another if they are best positioned to do so. Moreover, these authorities are time-limited. In fact, the relevant Department of Homeland Security and Department of Justice authority lapsed in October 2025; it is now only authorized through January 2026.

There is an urgent need to expand these limited authorities so that (i) appropriately trained state and local officials are given explicit authorization to engage in mitigation measures; (ii) there is explicit authorization for cross-agency support so

[11] House Amendment to S. 1071, United States Congress, (Dec. 7, 2025), https://thehill.com/wp-content/uploads/sites/2/2025/12/NDAA.pdf, §§ 8601-8607.

[12] *See* 6 U.S.C. § 124n; 10 U.S.C. § 130i; 50 U.S.C. § 2661.

that the most capable, best-resourced, and readily available trained entity can step in to respond to an active threat; and (iii) the requisite authorities are made permanent or, at a minimum, subject to long-term authorization.

Provisions included in the House-introduced 2026 NDAA would, if enacted into law, go a long way to addressing these issues, including by expanding federal authorities to engage in mitigation measures, granting mitigation authorities to trained state and local authorities, and setting a 2031 sunset, which puts all of these authorities on a longer term footing.[13]

b. Need for Additional Resources and Ongoing Research and Development

The exercise also highlighted a significant resource gap critical to effective mitigation. Even with expanded authorities, there are limited resources to address some of the most acute threats, including the kind of swarm attack that was highlighted in the exercise; threats posed by drones that operate outside of the spectrum band most readily captured by many detection tools; and drones that fail to emit any signal at all, such as fiber-optic drones.

The exercise highlighted the need for a nimble counter-UAS industry that can adapt and adjust to emergent threats, and for a system that enables authorized officials to employ technologies that match the threat.

4. Counter-UAS Efforts Need to Be Normalized as a Part of General Security and Crisis Management Planning

One of the most interesting aspects of the exercise is how the discussion about counter-drone crisis response merged into discussions of other forms of crisis response. Among the key needs are (i) effective coordination of the emergency response; (ii) backup energy supplies; (iii) effective, consistent, and coordinated internal and external communications; and (iv) cross-organizational support.

The exercise thus highlighted the ways in which C-UAS planning needs to be incorporated into all security and crisis management planning and the ways in which security and crisis management planning needs to consider the risk posed by drone-related threats.

[13] Id.

Conclusion

The exercise brought into sharp relief the scope and scale of the threat posed by the negligent and malicious use of drones, the gaps in resources and authorities, and key needs at the state and local level. The good news is that there are immediate opportunities for meaningful progress, including through expanded authorities, regulatory reforms, increased resourcing, and education and planning via the kinds of exercises conducted in Grand Forks. This is not a threat our country must face unprepared. We have the innovation and experience to build a more resilient homeland. Our policies, training, and resources need to—and can—evolve to meet the occasion.

Appendix A: *Participants*

The Center would like to extend our deepest thanks to Grand Sky for hosting the event, to DroneShield and P3 Tech Consulting for the support, and to the following individuals and entities for lending their time and expertise to the exercise:

Facilitators:

Bill Daggett
Delta Advisory Group

Jennifer Daskal
Venable LLP / Center for Cybersecurity Law and Policy

Davis Hake
Venable LLP / Center for Cybersecurity Law and Policy

Tim McGiff
Venable LLP / Center for Cybersecurity Law and Policy

Scott Meyer
Grand Sky

Participants:

- Altru Health System
- Apium Inc
- County of Grand Forks
- Curry & Co. Solutions LLC
- Customs and Border Protection
- Delta Advisory Group
- DroneShield
- General Atomics Aeronautical Systems, Inc. (GA-ASI)
- Grand Forks and East Grand Forks Chamber of Commerce
- Grand Forks Police Department
- Minnkota Power Cooperative
- Motorola Solutions
- NDeavor
- Nodak Electric Cooperative
- North Dakota Department of Commerce
- North Dakota House of Representatives
- North Dakota Information Technology
- North Dakota Legislature
- North Dakota National Guard
- North Dakota Petroleum Council
- North Dakota Public Service Commission
- North Dakota Transmission Authority
- Northern Plains UAS Test Site
- Northrop Grumman Corporation
- Phalanx Defense
- SkySafe
- The Office of Congresswoman Julie Fedorchak
- University of North Dakota
- University of North Dakota Alumni Association Foundation

Appendix B: *Scene Setter*

Global Outlook

Global geopolitical tensions and economic upheaval have fueled animosity toward the United States. International terrorist groups have been increasingly vocal in condemning the U.S. for inciting conflict and unrest across the globe and have increasingly advocated for unspecified attacks on Americans and on the U.S. homeland.

Tensions with the People's Republic of China ("PRC") are high, given increased technological and security cooperation between the United States and Taiwan. Credible reporting indicates that Iran is considering ways to retaliate against the United States for the 12 days of bombing in July 2025, while also continuing to explore new ways to retaliate against the United States for the 2020 killing of IRGC Commander Qasem Soleimani—to include the possible use of proxies to conduct terrorist attacks. Russia has doubled down on rhetoric that NATO is de facto at war with Russia.

The Department of Homeland Security and Federal Bureau of Investigation have issued several bulletins over the past 3 months warning that critical infrastructure owners and operators and large-scale public gatherings are potential targets by foreign and domestic extremists and urging increased precautions.

Overview - Minor Spoon, North Dakota

Minor Spoon is a small city of roughly ~70,000 permanent residents located a few miles away from the border of North Dakota and Minnesota. Within a 20 mile radius of the city center is an international airport, university, a coal power plant, and an Air Force Base. Minor Spoon's government is well resourced and possesses strong relationships with the community and state government entities.

Local Outlook - Minor Spoon, North Dakota

Over the past week, there have been numerous unverified public reports (local news and social media) of an unusual number of drone sightings in the Minor Spoon area. This is starting to be picked up on national news, and the governor and mayor's office have been fielding calls from concerned citizens.
Earlier in the month, the Cybersecurity and Infrastructure Security Agency ("CISA") alerted civilian critical infrastructure owners and operators across the Midwest to warn them of what appears to be increased cyber activity/attempts to penetrate their networks.

Two days ago, the local FBI field office reached out to campus security officers across the United States, warning of increased online chatter expressing support for an attack that targets students. No specific threat actors or targets have been identified.

Appendix C: *Center for Cybersecurity Policy and Law Drone Project*

The Center for Cybersecurity Policy and Law is a nonprofit 501(c)(6) organization that develops, advances, and promotes best practices and educational opportunities among homeland security and cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of industry, civil society, and government entities. To learn more about the Center generally and our wide-ranging initiatives, please visit https://centerforcybersecuritypolicy.org. And to learn more about the Center's specific drone-related work, contact Jennifer Daskal, jdaskal@venable.com.

Co-Host

GRANDSKY
GRAND FORKS COUNTY, ND

Supporters and Sponsors

DRONESHIELD

TECH CONSULTING
PEOPLE · PLATFORMS · POLICY